MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

ISO 27001
LL-C (Certification)

Politika řízení vztahů s dodavateli

Zpracoval	**Odbor kybernetické bezpečnosti a koordinace ICT**
Ověřil	**Manažer kybernetické bezpečnosti**
Schválil	**Náměstek ministra vnitra pro řízení sekce ICT**

datum schválení: **20.09. 2017**

Stav:	**Schválený**	Klasifikace:	**Interní**
Verze:	**3**	Počet stran:	**11**
Platnost:	**20.09. 2017**	Účinnost:	**20.09. 2017**

ISMS 03.01.01 Politika řízení vztahů s dodavateli

Obsah

OBSAH **2**
1. ÚČEL **3**
2. STANOVENÍ BEZPEČNOSTNÍCH POTŘEB **4**
2.1. PRAVIDLA VÝBĚRU DODAVATELŮ 4
2.2. BEZPEČNOSTNÍ PODMÍNKY STANOVENÉ VE SMLOUVÁCH S DODAVATELI 5
3. POSKYTOVÁNÍ INFORMACÍ **8**
4. ŘÍZENÍ VZTAHŮ S DODAVATELI **9**
5. HODNOCENÍ DODAVATELŮ **10**
5.1. ZÁKLADNÍ HODNOCENÍ 10
5.2. PROVÁDĚNÍ ZÁKAZNICKÝCH AUDITŮ 10
6. VŠEOBECNÉ INFORMACE **11**
6.1. ZKRATKY, POJMY A DEFINICE 11
6.2. DOTČENÍ ZAMĚSTNANCI 11
6.3. SOUVISEJÍCÍ DOKUMENTY 11

1. Účel

Účelem tohoto vrcholového dokumentu je nastavení zásad pro řízení vztahů s dodavateli, které zohledňují potřeby řízení bezpečnosti informací u dodavatelů nebo jiných osob, které se podílejí na rozvoji, provozu nebo zajištění bezpečnosti informačních nebo komunikačních systémů spadajících pod zákon č. 181/2014 Sb., o kybernetické bezpečnosti ve znění pozdějších předpisů. Ošetřuje také způsob jejich vyhodnocování a správy v souladu s implementací požadavků ZoKB a vyhlášky č. 316/2014 Sb., o kybernetické bezpečnosti, ve znění pozdějších předpisů. Předpis stanovuje zásady pro řízení vztahů s dodavateli také v souladu se zákonem č. 365/2000 Sb., o infomačních systémech veřejné správy a o změně některých dalších zákonů, se zákonem č. 101/2000 o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů a zákonem č. 134/2016 Sb., o zadávání veřejných zakázek (dále jen ZoVZ).

2. Stanovení bezpečnostních potřeb

Pro dodávky produktů a služeb, které se předmětně vztahují k aktivům ISMS, resort MV stanovuje a hodnotí bezpečnostní potřeby na základě měření a řízení rizik a návrhu opatření v rámci periodických a mimořádných hodnocení rizik a návrhů opatření v rámci ISMS. Na základě uvedených hodnocení resort MV stanovuje bezpečnostní potřeby ve vztahu k jednotlivým nebo souborným aktivům, včetně těch, jež jsou zajišťovány dodávkami nebo službami třetích stran. Při výběru zboží a služeb resort MV respektuje v souladu s ZoISVS Informační koncepci České republiky, byla-li vydána.

Zadavatel se při zadávání a v průběhu veřejné zakázky řídí zákonem č. 134/2016 Sb., o zadávání veřejných zakázek, a nařízením Ministerstva vnitra č. 45 ze dne 23. listopadu 2016 o zadávání veřejných zakázek.

2.1. Pravidla výběru dodavatelů

Resort MV v rámci výběru dodavatelů zboží a služeb, které jsou předmětné k aktivům ISMS, zohledňuje identifikované bezpečnostní potřeby v souladu s příslušnými právními předpisy pro zadávání zakázek, při zachování podmínky hospodářské soutěže a konkurenčního prostředí mezi dodavateli a bezpečnostní potřeby formou jednotlivých požadavků zahrne do smlouvy, kterou s dodavatelem uzavírá. Zohlednění požadavků vyplývajících z bezpečnostních opatření v míře nezbytné pro splnění povinností podle ZoKB nelze považovat za nezákonné omezení hospodářské soutěže nebo neodůvodněnou překážku hospodářské soutěži.

Omezující požadavky na výběr dodavatelů začleňuje resort MV do zadávacích podmínek výběru, přičemž:

- Každý takový požadavek v celém svém rozsahu odpovídá bezpečnostním opatřením schváleným v rámci ISMS, tj. nesmí překračovat potřeby resortu MV v oblasti řízení bezpečnosti informací stanovené těmito bezpečnostními opatřeními.
- Vzhledem k účelu daného zadávacího řízení a vzhledem k jeho konkrétním okolnostem nesmí rozsah takového požadavku překračovat míru nezbytnou pro splnění povinností resortu MV, tj. míru nezbytnou pro realizaci schválených bezpečnostních opatření.
- Je-li odůvodněné, podle předmětu dodávky zadavatel stanoví požadavky na osvědčení uchazeče podle zákona 412/2005 Sb., o ochraně utajovaných informací a bezpečnostní způsobilosti, ve znění pozdějších předpisů.
- Podle předmětu dodávky zadavatel stanoví technické kvalifikační požadavky včetně požadavků na certifikace a kvalifikace pracovníků, kteří se budou podílet na dodávce,

Výběrem dodavatele musí být rovněž minimalizována případná rizika, která by mohla nastat při nevhodném výběru dodavatele zejména z důvodu jeho nezpůsobilosti splnit předmět veřejné zakázky, a to:

- Riziko ekonomické a finanční nezpůsobilosti požadavkem na předložení čestného prohlášení uchazeče o jeho způsobilosti.

- Riziko nevhodné technické kvalifikace vhodným nastavením technických kvalifikačních předpokladů.
- Riziko nedostatečné součinnosti dodavatele po realizaci dodávky, tj. v reálném provozu, a to jasnou deklarací zodpovědnosti dodavatele za parametry jím poskytované smluvní podpory, včetně závazku poskytovat mimořádně vysokou míru součinnosti, zajištěného termíny a sankcemi.

Resort MV požaduje splnění základních a profesních kvalifikačních předpokladů i u předmětných veřejných zakázek malého rozsahu, které jinak standardnímu zadávacímu řízení dle ZoVZ nepodléhají.

Před uzavřením smlouvy s vybraným uchazečem provádí zadavatel hodnocení rizik podle přílohy č. 2 k VyKB.

2.2. Bezpečnostní podmínky stanovené ve smlouvách s dodavateli

Zadavatel jako součást zadávacích podmínek předloží uchazečům obchodní a platební podmínky plnění veřejné zakázky ve formě závazného textu návrhu smlouvy, jehož znění uchazeči nebudou oprávněni měnit a doplňovat na jiných než výslovně označených místech.

Dále zadavatel stanoví ve smlouvě podle předmětu dodávky požadavky v souladu se zákonem č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů, a to především požadavky uvedené v § 13 -15 tohoto zákona.

V případech, kdy předmětem plnění smlouvy není jen jednorázová dodávka, ale dlouhodobější poskytování služby – jedno zda např. „jen“ podpory (maintenance) dodaných licencí nebo na zakázku vyvinuté SW aplikace, či provozování infrastruktury nebo systému (informačního nebo komunikačního), je nezbytné zajistit, aby předmět smlouvy byl stanoven maximálně komplexně formou konkrétních ujednání o úrovni všech poskytovaných služeb, tzv. SLA. V případě, že se jedná o dodavatele na provozovatele informačních nebo komunikačních systémů dle ZoKB je potřeba, aby zadavatel (nebo pověřená osoba) sjednal ve smlouvě právo na informace a data, která pro ně provozovatel uchovává, včetně kontroly uchovávaných informací a dat v reálném čase.

Zadavatel zakázky má povinnost mít smluvně zajištěny zejména následující práva a povinnosti:

- V rámci ujednání o bezpečnosti informací zejména:
  - ✓ obecná povinnost dodavatele zachovávat mlčenlivost a dodržovat zásady bezpečnosti informací zadavatele,
  - ✓ povinnost dodavatele dodržovat zásady bezpečnosti informací dle požadavků zadavatele,
  - ✓ stanovení úrovně ochrany dat a informací,
  - ✓ podmínky ukončení smluvního vztahu z důvodu bezpečnosti,
  - ✓ povinnost dodavatele poskytovat zadavateli součinnost při plnění jeho povinností podle ZoKB a jeho prováděcích předpisů, a to včetně preventivních aktivit,

- ✓ povinnost dodavatele poskytovat zadavateli součinnost při plnění jeho povinností vyplývajících z rozhodnutí státních orgánů vykonávajících působnost na úseku kybernetické bezpečnosti.

➢ V rámci ujednání o úrovni služeb zejména zajistit, že dodavatel bude schopen dodržovat veškerá bezpečnostní opatření vyplývající z ZoKB.

➢ V rámci ujednání o soukromoprávním kontrolním režimu zejména:

- ✓ povinnost dodavatele podrobit se kontrolní činnosti zadavatele za účelem kontroly dodržování bezpečnostních opatření, které vyžaduje schválené ISMS, ZoKB a VyKB,
- ✓ povinnost dodavatele odstranit nedostatky zjištěné při této kontrolní činnosti.

Sjednané povinnosti dodavatele zajistí zadavatel ve smlouvě vhodnými právními prostředky (smluvní pokuta aj.).

Pokud se dodavatel stává povinnou osobou podle ZoKB, zadavatel ho o tom neprodleně a prokazatelně informuje. Zadavatel v takovém případě podle předmětu plnění smlouvy identifikuje podle kterého písmene § 3 ZoKB je dodavatel orgánem nebo osobou povinnou podle ZoKB a podle tohoto zařazení smluvně zajistí veškeré povinnosti příslušného dodavatele podle ZoKB a VyKB formou SLA, kde stanoví konkrétní požadavky, termíny a sankce v případě neplnění.

Konkrétní termíny jsou ve smlouvě stanoveny i tehdy, pokud ZoKB nebo VyKB používá obecný termín bezodkladně nebo bez zbytečného odkladu.

Dále zadavatel ve smlouvě stanoví:

➢ přiměřeným způsobem podle předmětu plnění veřejné zakázky konkrétně obsah bezpečnostních opatření, obsah a strukturu bezpečnostní dokumentace,

➢ popis dat, provozních údajů a informací, které má provozovatel k dispozici v souvislosti s provozováním systému a které má na žádost zadavatele v dohodnutém termínu předat nebo případně sjednaným způsobem zlikvidovat nadbytečné kopie,

➢ výši a podmínky úplaty na pokrytí nutných výdajů za zavedení bezpečnostních opatření podle ZoKB dále pro případ předání dat, provozních údajů a informací a zničení nepotřebných kopií,

➢ povinnost dodavatele nahradit zadavateli veškeré škody, které by dodavatel zadavateli způsobil neplněním svých smluvních povinností, včetně dodavatelem způsobených sankcí uložených zadavateli ze strany NUKIB nebo jiných kontrolních orgánů.

Je-li aplikovatelné (v případě služeb cloud computingu je tento požadavek povinný podle ZoKB), zadavatel sjedná s dodavatelem také postup a termíny pro hlášení kybernetických bezpečnostních incidentů, hlášení a aktualizaci kontaktních údajů, provádění reaktivních, ochranných opatření, opatření obecné povahy a plnění rozhodnutí o uložení povinnosti ze strany NUKIB.

Je-li předmětem dodávky služba cloud computingu, zadavatel dále stanoví:

- systém schvalování subdodavatelů služby cloud computingu,
- řízení kontinuity činností v souvislosti s poskytovanou službou cloud computingu,
- určení vlastníka uchovávaných dat,
- stanovení úrovně ochrany dat z pohledu důvěrnosti, dostupnosti a integrity.

3. Poskytování informací

V souladu se ZoKB se informace, jejichž zpřístupnění by mohlo ohrozit zajišťování kybernetické bezpečnosti nebo účinnosti opatření vydaného podle tohoto zákona, nebo informace, které jsou vedené v evidenci incidentů, ze kterých by bylo možné identifikovat orgán nebo osobu, která kybernetický incident ohlásila, se podle předpisů upravujících svobodný přístup k informacím neposkytují.

4. Řízení vztahů s dodavateli

Resort MV uplatňuje v rozsahu pravidel ISMS zejména následující zásady pro řízení vztahů s dodavateli:

- Stanovení jednoznačných závazků a povinností dodavatelů, které jednoznačně definuje (optimálně formou SLA) předmět plnění dodávky, včetně způsobů sledování plnění a kritérií pro jejich jednoznačné vyhodnocení,
- Aplikace procesů kontroly zahrnuje:
  - ✓ způsoby předávání výsledků kontrol (komunikační cesty, dokumentové formáty, uznávané certifikáty atp.),
  - ✓ opatření pro případ nesplnění povinností, tj. nastavení kompetentní role (osoby), lhůty pro odezvu a případné postihy.

5. Hodnocení dodavatelů

Hodnocení konkrétních dodavatelů pro kontrolu plnění požadavků v oblasti kybernetické bezpečnosti má na starosti zaměstnanec resortu MV odpovědný za daný smluvní vztah. Reporty hodnocení dodavatelů (dodržování SLA) předává v pravidelných intervalech, minimálně jednou ročně, příp. na vyžádání OKB.

5.1. Základní hodnocení

Základním způsobem hodnocení dodavatelů je vyhodnocení platných a probíhajících smluvních vztahů, nastavených SLA a dále zejména:

- Dodací termíny.
- Množství reklamací.
- Úroveň komunikace.
- Zavedené systémy managementu (ISO).
- Hodnocení z hlediska ZoKB a prováděcích předpisů.

5.2. Provádění zákaznických auditů

Resort MV požaduje u klíčových služeb a dodávek, přístup k informacím o dodávce a dodavateli prostřednictvím provedení zákaznického auditu v intencích ČSN EN ISO 19011:2012, který realizuje vlastními silami nebo prostřednictvím pověřené třetí strany. Rozsah auditu je dán požadavky na daného dodavatele dle struktury dodávek či poskytovaných služeb. V případě služeb cloud computingu je požadavek zákaznického auditu povinný podle ZoKB. Základními referenčními normami pro kontrolu bezpečnostních opatření jsou ČSN ISO/IEC 27001:2014, ZoKB a prováděcí předpisy. Má-li dodavatel zavedený a nezávislým certifikačním orgánem certifikovaný systém bezpečnosti informací dle normy ČSN ISO/IEC 27001:2014 (minimálně pro rozsah poskytovaných služeb), je možné k tomuto při provádění zákaznického auditu přihlédnout, nikoliv však touto certifikací nahradit provedení celého zákaznického auditu.

6. Všeobecné informace

6.1. Zkratky, pojmy a definice

Zkratky, pojmy a definice jsou obsahem dokumentu:

- ***ISMS 02.03.02 Zkratky a pojmy ISMS MV***.

6.2. Dotčení zaměstnanci

Tento dokument je určen pro všechny zaměstnance a externí pracovníky, kteří se podílejí na přípravě nebo zajištění dodávek produktů a služeb, jež se svou předmětnou povahou dotýkají aktiv ISMS MV.

6.3. Související dokumenty

- ***ISMS 0.50.50 Nařízení MV č. 40-2012 o resortních pravidlech centralizovaného zadávání a centrálního nákupu***,
- ***ISMS 0.50.52 Nařízení MV č. 45-2016 o zadávání veřejných zakázek***,
- ***ISMS 0.50.08 Pokyn MV č. 6-2012, kterým se ukládá evidovat a zveřejňovat uzavřené smlouvy***,
- ***ISMS 0.50.54 Nařízení MV č. 45-2011 o řízení, organizaci a výkonu ekonomické činnosti***.